UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

DISH NETWORK, L.L.C.,
ECHOSTAR TECHNOLOGIES, L.L.C.
and NAGRASTAR, L.L.C.,

Plaintiff,

v. Case No. 09-C-428

KELLY STAFFORD, INFINITY SYSTEMS USA, LLC,
d/b/a ISUSA.biz, INFINITY SYSTEMS, LLC,
FRANK KOCKEN, GERALD "JERRY" PAHL,
CORY KOCKEN and KOCKEN TECHNOLOGIES, LLC,

Defendants.

ORDER GRANTING TEMPORARY RESTRAINING ORDER AND CIVIL SEIZURE/IMPOUNDMENT ORDER AND ORDER FOR DEFENDANTS TO SHOW CAUSE WHY PRELIMINARY INJUNCTION SHOULD NOT ISSUE

Having considered Plaintiffs' *Ex Parte* Motion for Temporary Restraining Order and Civil Seizure/Impoundment Order, the Plaintiffs' Memorandum in Support of Plaintiffs' *Ex Parte* Motion for Temporary Restraining Order, and Civil Seizure/Impoundment Order, the Declaration of Kevin Gedeon, the Declaration of Jerry Lee Gee, the Declaration of Daniel McMullen, the Declaration of Scott Anderson, the Declaration of John M. McLaughlin and the complete file of this Action, the Court finds:

1. The Plaintiffs will be injured by the Defendants through any further sale and/or distribution of satellite piracy devices allowing for the unauthorized interception of the Plaintiffs' signals without payment;

2. The damage to the Plaintiffs is irreparable in that once the sales of piracy devices are made to third parties, the damages caused by same are incalculable and significant;

3. This order should be granted without notice in that, given the brazen manner in which it appears the defendants have violated federal law prohibiting the unauthorized interception of Plaintiffs' satellite signals, I conclude that the defendants are the type of defendants who would take actions to remove or damage evidence should they be given notice. I also find from the evidence submitted that the device or products that are designed and used to intercept Plaintiffs' signal, as well as paper and/or electronically stored records relating to their sale and use, are susceptible to easy and quick destruction or concealment, and that once destroyed or concealed, it may be impossible to determine the extent of Plaintiffs' damages and prevent further damages in the future.

4. The damage to the Defendants from issuance of a temporary restraining order enjoining them from continuing to sell devices and programing that assists others to circumvent the encryption protection contained in the software on NagraStar's smart cards or contained within EchoStar Technologies' receivers or any other technological measure adopted by DISH Network and/or EchoStar Technologies and/or NagraStar in violation of federal law is of no consequence since they have no lawful right to engage in such conduct. Although authorizing entry into the Defendants' premises to seize and impound the device and products involved in the

violations of federal law alleged in the complaint and related evidence is an extraordinary interlocutory remedy, I conclude that it is warranted under the specific facts and circumstances of this case. In particular, I have relied upon the clear evidence of ongoing and deliberate violations of federal law by the Defendants; the irreparable harm to the Plaintiffs caused by the ongoing loss of revenue resulting from the Defendants' pirating activities; the inherent susceptibility of the devises and evidence sought by the Plaintiffs to destruction and/or concealment, especially by individuals with the technological skill and training of the Defendants; and the severe sanctions available under the law for violations of the type alleged which would provide a strong incentive for the Defendants to make such evidence disappear if they are permitted the opportunity to do so.

5. The public's interest is also served by issuance of this order since, if the allegations are true, the Defendants are showing a shocking and blatant disregard for the rule of law and enabling many others to do the same. The public's interest is served by enforcement of the law.

6. That other good cause has been shown and the Court hereby GRANTS Plaintiffs' Motion as follows:

> The Defendants, Defendants, Kelly Stafford and Infinity Systems USA, LLC d/b/a "ISUSA", Infinity Systems, LLC, Frank Kocken, Gerald "Jerry" Pahl, Cory Kocken and Kocken Technologies, LLC (collectively, "Defendants") and their employees, agents, representatives, and all other persons acting or claiming to act on their behalf or under Defendants' direction or authority, and all persons acting in concert or in participation with Defendants are hereby ENJOINED from:

A. Manufacturing, importing, offering to the public, providing, modifying, or otherwise trafficking in any so called "Free to Air" ("FTA") receiver or EchoStar Technologies receiver that has been modified without authorization, any NagraStar smart cards that have been modified without authorization, any DISH Network satellite pirating device regardless of form, including smart cards that have been programmed with DISH Network pirate software, or any other technology, product, service, device, component, or part thereof, including any device for utilization with Control Word Sharing or IKS technology, that:

i. is primarily designed or produced for the purpose of circumventing the encryption protection contained in the software on NagraStar's smart cards or contained within EchoStar Technologies' receivers or any other technological measure adopted by DISH Network and/or EchoStar Technologies and/or NagraStar that effectively controls access to copyrighted programming or effectively protects the exclusive rights afforded the owners of copyrighted programming;

ii. has only limited commercially significant purpose or use other than to circumvent DISH Network's encryption access control protection or any other technological measure adopted by DISH Network, EchoStar Technologies and/or NagraStar that effectively controls access to copyrighted programming or effectively protects the exclusive rights afforded the owners of copyrighted programming;

iii. is knowingly marketed by Defendants and/or others acting in concert with them for use in circumventing DISH Network's encryption access control protection or any other technological measure adopted by DISH Network and/or EchoStar Technologies and/or NagraStar that effectively controls access to copyrighted programming or effectively protects the exclusive rights afforded the owners of copyrighted programming.

B. Assembling, modifying, selling, advertising, marketing, possessing, transporting, and/or distributing through any means any FTA receiver, EchoStar Technologies receiver or NagraStar smart card that has been modified without authorization or any other electronic, mechanical, or other devices, including smart cards, FTA receivers that have been programmed with pirate software, the pirate software itself, the design of which renders them primarily useful for the purpose of the surreptitious interception of electronic communications including DISH Network's signals.

C. Assembling, modifying, selling, advertising, marketing, possessing, transporting and/or distributing through any means any type of FTA receivers, including, but not limited to, FTA receivers with smart card readers installed and including, but not limited to, FTA receivers with an Ethernet port attachment which allows for a continual direct Internet connection with the FTA receiver such as the "Nfusion" receiver or FTA receiver or so-called "dongle" designed or modified or programmed for utilization with IKS technology, where the Defendants or those acting with the Defendants are:

i. selling or distributing FTA receivers that are already pre-programmed with DISH Network pirate software;

ii. selling or distributing FTA receivers or other devices that are designed or modified or programmed for use with IKS;

iii. programming the FTA receivers with DISH Network pirate software before distribution to the FTA receiver customers;

iv. distributing, in any manner, the DISH Network piracy software to the FTA receiver customers and others including, but not limited to, distributing the DISH Network piracy software by e-mail attachments or distributing the DISH Network piracy software by delivering the software contained on a software holding device;

v. directing, in any way, the FTA receiver customers to piracy websites, piracy forums, and/or piracy chat rooms where the DISH Network pirate software is available (pirate websites);

vi. operating, either directly or indirectly piracy websites, piracy forums, and/or piracy chat rooms where the DISH Network pirate software is available (pirate websites);

vii. intentionally utilizing third parties to effectuate having the FTA receiver customer's FTA receiver ultimately programmed with DISH Network piracy software;

viii. subsidizing the pirate websites, including subsidizing the pirate websites through advertising on the pirate websites;

ix. utilizing website hyperlinks back and forth between any websites operated or controlled by Defendants and the piracy websites;

x. selling or distributing peripheral devices which are of assistance to the FTA receiver customers to effectuate the unauthorized interception of DISH Network signals, including but not limited to card readers and dish antennas which are designed to receive premium channels satellite signals as opposed to true FTA signals.

D. Destroying, hiding or removing all records, in any form (including electronic form), that evidence, refer, or relate to FTA Receivers, modified FTA receivers, FTA receivers and related technology that are designed, modified and/or programmed for use with IKS, DISH Network piracy software, altered or modified NagraStar smart cards, smart cards that have been programmed with pirate software, receivers, so called "virgin" smart cards, or other unlawful devices and any components thereof, as described herein; communications or correspondence with suppliers, including any suppliers of FTA receivers or DISH Network piracy software or customers of pirating devices, software, hardware or other equipment, or services or know-how concerning smart card programming, box key extraction and DISH Network signal piracy; the identity of any manufacturers or suppliers including any suppliers of FTA receivers or customers of smart card programming, box key extraction devices, or receiver modification programming services; and the quantity of all such devices in inventory and sold by Defendants; and

E. Obligating the Defendants to immediately cease operation of the violate other terms of the requested injunctive relief set forth website www.isusa.biz in any manner such that the operation would herein.

THEREFORE IT IS ORDERED that the Plaintiff's Motion for Civil Seizure/Impoundment Order is **GRANTED** and the Court shall issue two Writs of Seizure as follows:

The Clerk of the Court shall deliver to the United States Marshal or other suitable officers this Order and two Writs of Seizure directing the United States Marshal or other suitable officers to execute same at the Infinity Systems USA Green Bay Wisconsin store located at 3134 Holmgren Way, Green Bay, Wisconsin and at the Kocken Technologies, LLC Principal Office located at 7607 Blake Road, Greenleaf, Wisconsin and to:

1. Impound all FTA receivers, FTA receivers and related hardware and software that are designed, modified and/or programmed for use with IKS, and/or modified FTA receivers and/or peripheral devices related to the FTA receivers such as card readers and dish antennas not designed to receive true FTA signals and/or DISH Network piracy software, including any devices holding and/or containing said software, DISH Network's, EchoStar Technologies' and/or NagraStar's smart cards, receivers, and/or signal theft devices that have been modified or manufactured without authorization, reprogramming equipment, and equipment used in the alteration and/or modification of said devices, and so called "virgin" smart cards that are in the possession, custody, or control of Defendants or their employees, agents, representatives and all other persons acting or claiming to act on their behalf or under Defendants' direction or authority, and all persons acting in concert or in participation with Defendants;

2. Impound all records, in any form (including electronic form), that evidence, refer, or relate to FTA receivers, FTA receivers and related hardware and software that are designed, modified and/or programmed for use with IKS, modified FTA receivers, DISH Network piracy software, peripheral devices related to the FTA receivers such as card readers and dish antennas not designed to

receive true FTA signals, altered or modified NagraStar smart cards, smart cards that have been programmed with pirate software, receivers, FTA receivers, so called "virgin" smart cards, or other unlawful devices and any components thereof, as described herein; communications or correspondence with suppliers, including any suppliers of FTA receivers, or customers of pirating devices, software, hardware or other equipment, or services or know-how concerning smart card programming, box key extraction, and DISH Network signal piracy; the identity of any manufacturers, suppliers, including any suppliers of FTA receivers or customers of smart card programming, box key extraction devices or receiver modification programming services; and the quantity of all such devices in inventory and sold by Defendants.

3. Impound all computers or electronic storage drives or back-up tapes in the possession, custody, or control of Defendants or their employees, agents, representatives, and all other persons acting or claiming to act on their behalf or under Defendants' direction or authority, and all persons acting in concert or in participation with Defendants that contain information related to Defendants' sales of FTA receivers, FTA receivers and related hardware and software that are designed, modified and/or programmed for use with IKS, modified FTA receivers, DISH Network piracy software, peripheral devices related to the FTA receivers such as card readers and dish antennas not designed to receive true FTA signals, unlawfully altered or modified DISH Network and/or NagraStar smart cards, EchoStar Technologies receivers, or any other unlawful devices or services as described herein with the Defendants retaining the right to move this Court to seek return of said computers only after the Plaintiffs are given sufficient time to examine the contents of same and at their option to make mirror image copies of any computer or electronic storage drives or back up tapes. To the extent it is reasonably practical to do so, Plaintiffs are to make mirror image copies of the hard drives of the above-described computers so as not to disrupt the legitimate business operations of the Defendants.

The Plaintiffs and/or their agents and/or their attorneys and/or persons under their supervision shall accompany the United States Marshal or other suitable officers and his or her deputies at the seizures, and the Plaintiffs and/or their agents and/or their attorneys and/or persons

under their supervision shall identify and inventory the items that are seized pursuant to the Writs of Seizure. The United States United States Marshal or other suitable officers are authorized:

1. To take inventory of above referenced items at the seizure of the items and grant possession of same to the Plaintiffs and/or their attorneys who shall act as substitute custodian and who shall inventory and store the seized items in a secure manner pending a further order of this Court. A suitable secure facility shall include the offices of the Plaintiffs' local counsel;

2. To utilize all due force necessary to execute this Court's order and to protect the Plaintiffs and their agents while executing the Impoundment Order; that necessary force shall include the authority to:

    a. Temporarily confiscate any weapons located at the Infinity Systems USA Green Bay, Wisconsin store located at 3134 Holmgren Way, Green Bay, Wisconsin and at the Kocken Technologies, LLC Principal Office located at 7607 Blake Road, Greenleaf, Wisconsin at least until the Plaintiffs and their agents and Attorneys have fully executed the Writs of the Seizure and left the Defendants' two premises;

    b. Break open and enter the Infinity Systems USA Green Bay, Wisconsin store located at 3134 Holmgren Way, Green Bay, Wisconsin and at the Kocken Technologies, LLC Principal Office located at 7607 Blake Road, Greenleaf, Wisconsin regardless of whether said premises are locked or unlocked, or occupied or unoccupied, and inspect the contents of any room, closets, cabinets, vehicles, containers, packages, or desks and seize any equipment utilized to manufacture the infringing items.

Plaintiffs are required to post a bond of $50,000. Plaintiffs are also to pay statutory costs and fees of the United States Marshal's Service.

AND FURTHER ORDERING that the Defendants appear on **May 5, 2009, at 9:30 a.m.** for a hearing to show cause:

1. Why the items seized should not be impounded pending the trial in this Action; and

2. Why this Temporary Restraining Order should not be confirmed as a Preliminary Injunction in this Civil Action.

Issued this 28th day of April, 2009 at 2:00 p .m.

s/ William C. Griesbach
William C. Griesbach
United States District Judge